Corps finis

Exercice 1.— $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$. $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$.

Exercice 2.— Commençons par construire un polynôme irréductible de degré 2 sur $\mathbf{F}_3$. Par exemple $\mathrm{P} = \mathrm{X}^2 + \mathrm{X} - 1$ convient, puisqu'il n'a pas de racines. Alors $\mathbf{F}_9 \simeq \mathbf{F}_3[\mathrm{X}]/(\mathrm{P})$, et de là, les tables sont faciles à écrire, en prenant une base de $\mathbf{F}_9$ sur $\mathbf{F}_3$ (par exemple $(1, \bar{\mathrm{X}})$.

Pour $\mathbf{F}_{16}$, il faut construire un polynôme irréductible de degré 4. La méthode est expliquée dans le cours.

Exercice 3.— Nous savons que $\mathbf{F}_q^\times$ est isomorphe à $\mathbf{Z}/(q-1)\mathbf{Z}$, donc en particulier, il possède $\varphi(q-1)$ générateurs.

Exercice 4.—

1. Commençons par remarquer que le centre de A est $\{x \in \mathrm{A} : xy = yx, \forall y \in \mathrm{A}\}$. Puisqu'il est commutatif par définition, et que tous les autres axiomes d'un corps sont vérifiés dans une algèbre à division, c'est un corps inclus dans A. Il est donc fini et de cardinal q, où q est une puissance d'un nombre premier p.
   Mais A peut être munie d'une structure de k-espace vectoriel, qui sera nécessairement de dimension finie par cardinalité : A est de cardinal q^n, avec $n \in \mathbf{N}$.
2. Puisque A est intègre, $\mathrm{A} - \{0\}$ agit sur lui-même par conjugaison. Mais si $x \in \mathrm{A} - \{0\}$, le stabilisateur de x (auquel on ajoute 0) est l'ensemble des $y \in \mathrm{A}$ tels que $xy = yx$. Ainsi, il est facile de voir que c'est un groupe abélien, mais aussi, en remarquant qu'il contient k, un k-espace vectoriel.
3. On applique la formule de classes pour l'action de $\mathrm{A} - \{0\}$ sur A tout entier. Alors, si $x \in k$, son orbite est réduite à un seul point, *i.e.* de cardinal $\frac{q^n-1}{q^n-1}$.
   Et si x n'est pas dans k, alors $\mathrm{Stab}_x \cup \{0\}$ est un sous-espace vectoriel strict de A, et donc de cardinal q^d. Donc son orbite est de cardinal $\frac{q^n-1}{q^d-1} \in \mathbf{N}$.
   Or, on vérifie que si $d \nmid n$, alors $(q^d-1) \nmid (q^n-1)$. En effet, si $n = da + r$ avec $0 < r < d$, alors $q^n - 1 = q^r(q^{ad} - 1) + q^r - 1$, et alors $q^d - 1 \mid q^r - 1$, ce qui est absurde.
4. On connait la formule suivante sur les polynômes cyclotomiques : $\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X})$. En particulier, $q^n - 1 = \prod_{d|n} \Phi_d(q)$.
   Mais de même, $q^d - 1 = \prod_{d'|d} \Phi_{d'}(q)$. On en déduit que
   $$\frac{q^n - 1}{q^d - 1} = \prod_{\substack{d'|n \\ d' \nmid d}} \Phi_{d'}(q) \in \mathbf{Z}.$$
5. La formule des classes appliquées à l'action de $\mathrm{A} - \{0\}$ sur lui-même nous donne alors :
   $$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}.$$

où la somme porte sur les orbites non réduites à un point, donc sur des $d < n$.
On en déduit que $\Phi_n(q)$ divise $q-1$, et donc $\Phi_n(q) \leq q-1$.
Mais si on note ζ_i les racines de Φ_n, qui sont toutes des racines de l'unité, on a

$$|\Phi_n(q)| = |\prod_{i=1}^{\varphi(n)} (q-\zeta_i)| \geq (q-1)^{\varphi(n)}.$$

On en déduit une contradiction dès que $n \geq 2$: donc $n = 1$ et A est bien un corps.

Exercice 5.—

1) Dans $\mathbf{F}_2[\mathrm{X}]$, on a $\mathrm{X}^4+1 = (\mathrm{X}+1)^4$ (penser au morphisme de Frobenius).
2) a) Les trois décompositions possibles sont obtenues en regroupant 2 par 2 les facteurs de degré 1, et sont

$$\mathrm{X}^4+1 = (\mathrm{X}^2+i)(\mathrm{X}^2-i) = (\mathrm{X}^2+\sqrt{2}\mathrm{X}-1)(\mathrm{X}^2-\sqrt{2}\mathrm{X}-1) = (\mathrm{X}^2+i\sqrt{2}\mathrm{X}-1)(\mathrm{X}^2-i\sqrt{2}\mathrm{X}-1).$$

   b) Le sous-groupe de $\mathbf{F}_p^*$ formé des carrés est d'indice 2, donc en particulier, le produit de deux non-carrés est un carré. Ainsi, si -1 et 2 ne sont pas des carrés, $-2 = (-1) \times 2$ est un carré, si 2 et -2 ne sont pas des carrés, $-1 = \frac{-2}{2}$ est un carré, etc.
   c) Si -1 est un carré dans $\mathbf{F}_p$, notons $\bar{i}$ une de ses racines. Alors $\mathrm{X}^4+1 = (\mathrm{X}^2+\bar{i})(\mathrm{X}^2-\bar{i})$, donc Φ_8 est réductible dans $\mathbf{F}_p[\mathrm{X}]$. De même si 2 ou -2 est un carré, en utilisant les deux autres décompositions de la question a).
3) a) Le critère d'irréductibilité par extension indique de Φ_8 est réductible si et seulement si il possède une racine dans une extension de degré inférieur ou égal à $\frac{4}{2} = 2$. Or $\mathbf{F}_p$ ne possède qu'une seule extension de degré 2, à savoir $\mathbf{F}_{p^2}$, d'où le résultat.
   b) Si Φ_8 possède une racine $\alpha \in \mathbf{F}_{p^2}$, alors cette racine vérifie $\alpha^4 = -1$, donc $\alpha^8 = 1$ et est donc d'ordre 8 dans $\mathbf{F}_{p^2}^*$. Ce groupe étant d'ordre p^2-1, on a bien que 8 divise p^2-1. Inversement, si 8 divise p^2-1, puisque $\mathbf{F}_{p^2}^*$ est cyclique, il existe un élement α d'ordre 8. Cet élément vérifie alors $\alpha^4 = -1$ (car sinon il serait d'ordre 4 et non pas 8).
   c) En raison des deux précédentes questions, il suffit de montrer que pour tout premier impair p, p^2-1 est divisible par 8. Or $p^2-1 = (p+1)(p-1)$. Ces deux nombres sont pairs, et l'un des deux doit être divisible par 4, d'où le résultat.

Exercice 6.— Supposons P irréductible. P est le polynôme minimal de chacune de ses racines, qui sont donc dans $\mathbf{F}_{q^d} \subset \overline{k}$, et vérifient $x^{q^d} = x$. Donc P divise $\mathrm{X}^{q^d} - \mathrm{X}$. Si P n'était pas premier à $\mathrm{X}^{q^{\frac{d}{p}}} - \mathrm{X}$, pour p facteur premier de d, alors ces deux polynômes auraient une racine en commun, qui serait alors dans $\mathbf{F}_{q^{\frac{d}{p}}}$. Une telle racine aurait alors un degré divisant $\frac{d}{p}$, ce qui est impossible puisqu'on vient de dire que toutes les racines de P étaient de degré d. Inversement, supposons que P vérifie les deux critères. Alors, puisque P divise $\mathrm{X}^{q^d} - \mathrm{X}$, toutes ses racines (dans $\overline{k}$) sont dans $\mathbf{F}_{q^d}$. On sait que les extensions intermédiaires de $\mathbf{F}_{q^d}/\mathbf{F}_q$ sont précisément les $\mathbf{F}_{q^n}$ sur $\mathbf{F}_q$, pour n divisant d. Si P avait une racine dans une extension de k de degré inférieur ou égal à $d/2$, cette racine serait donc nécessairement dans un $\mathbf{F}_{q^{\frac{d}{p}}}$, pour p divisant d. Mais alors P et $\mathrm{X}^{q^{\frac{d}{p}}} - \mathrm{X}$ auraient une racine commune et donc un pgcd non trivial, ce qui est contraire aux hypothèses. Donc P n'a de racines dans aucune extension de degré plus petit que $d/2$, et donc est irréductible.

Exercice 7.—

1. Si $h = 0$, alors on a $\mathrm{S}_q(0) = q = 0$. Si $q-1 \mid h$, et $h \geq 1$, pour tout $x \in \mathbf{F}_q^\times$, on a $x^h = 1$. On en déduit que $\mathrm{S}_q(h) = q-1$.
   Si $q-1$ ne divise pas h, le fait que $\mathbf{F}_q^\times$ soit cyclique d'ordre $q-1$ prouve qu'il existe $y \in \mathbf{F}_q^\times$ tel que $y^h \neq 1$. On a alors
   $$\mathrm{S}_q(h) = \sum_{x \in \mathbf{F}_q} x^h = \sum_{x \in \mathbf{F}_q} y^h x^h = y^h \mathrm{S}_q(h).$$
   On en déduit que $\mathrm{S}_q(h) = 0$.
2. S'il existe k tel que $f_k(x_1, \ldots, x_n) \neq 0$, alors $\prod_k (1 - f_k(x_1, \ldots, x_n)^{q-1}) = 0$ modulo p. Si pour tout k, on a $f_k(x_1, \ldots, x_n) = 0$, alors $\prod_k (1 - f_k(x_1, \ldots, x_n)^{q-1}) = 1$ modulo p. La congruence annoncée en découle.
3. On a
   $$\sum_{\underline{x} \in \mathbf{F}_q^n} x_1^{j_1} \cdots x_n^{j_n} = \prod_{l=1}^{n} \left(\sum_{x_l \in \mathbf{F}_q} x_l^{j_l} \right).$$
   Si $j_1 + \cdots + j_n < n(q-1)$, alors il existe k tel que $j_k < q-1$. Donc le k-ième facteur de ce produit est nul, et donc la somme aussi. On utilise ce résultat pour calculer $\sum_{\underline{x} \in \mathbf{F}_q^n} \prod_k (1 - f_k(x_1, \ldots, x_n)^{q-1})$. Le produit est une combinaison linéaire de sommes de monômes de degré inférieur ou égal à $d(q-1) < n(q-1)$. La somme est donc nulle dans $\mathbf{F}_q$, et donc $\mathrm{card}(\mathrm{V}) \equiv 0$ modulo p.
4. Soit N le nombre de zéros de P dans $\mathbf{F}_q^n$. On a $\mathrm{N} \equiv 0$ et $\mathrm{N} \geq 1$ puisque $(0, \ldots, 0)$ est un zéro. Il vient $\mathrm{N} \geq p$.
5. C'est le même raisonnement que précédemment.

Exercice 8.— L'unicité ne devrait pas être la partie difficile : si deux fonctions polynomiales de degré inférieur ou égal à $q-1$ sont égales, alors les polynômes possèdent q zéros communs, et sont donc égaux.
Pour l'existence, une astuce diabolique permet de conclure : si $f : \mathbf{F}_q \to \mathbf{F}_q$, alors f coïncide avec la fonction polynomiale définie par le polynôme
$$\sum_{a \in \mathbf{F}_q} f(a) \left(1 - (\mathrm{X} - a)^{q-1}\right).$$

Enfin, dans le cas de fonctions à plusieurs variables, on peut de même définir un polynôme satisfaisant les hypothèses de la manière suivante :
$$\sum_{(a_1, \ldots, a_n) \in \mathbf{F}_q^n} f(a_1, \ldots, a_n) \prod_{i=1}^{n} \left(1 - (\mathrm{X}_i - a_i)^{q-1}\right).$$

Exercice 9.— Soit G un groupe dont le groupe des automorphismes soit trivial. En particulier, les automorphismes intérieurs sont triviaux, et donc G est abélien.
Mais dans un groupe abélien, $x \mapsto x^{-1}$ est un automorphisme, donc ici, tout élément est égal à son propre inverse, *i.e.* d'ordre 2.
Un groupe abélien où tout élément est d'ordre 2 est un $\mathbf{F}_2$-espace vectoriel, et un automorphisme $\mathbf{F}_2$-linéaire n'est rien d'autre qu'un automorphisme du groupe.
Par l'axiome du choix, il existe une base de G en tant que $\mathbf{F}_2$-espace vectoriel, et permuter deux vecteurs de la base donne lieu à un automorphisme non trivial. Donc si Aut(G) est trivial, alors G est un $\mathbf{F}_2$-espace vectoriel de dimension 0 ou 1, et donc G est soit le groupe trivial, soit le groupe à deux éléments.